IN THE CLAIMS

This listing of the claim will replace all prior versions and listings of claim in the present application.

Listing of Claims

Claims 1-16 (canceled).

B1

17. (currently amended) ~~The~~ A method for performing authentication between a client and a service server connected over a network, comprising the steps of:

generating, by said client, a random number, ciphering said random number, and transmitting said random number thus ciphered to said service server;

deciphering, by said service server, said ciphered random number transmitted from said client, re-ciphering said random number thus deciphered, and transmitting said random number thus re-ciphered to said client; and

re-deciphering, by said client, said re-ciphered random number, confirming whether said random number thus re-deciphered coincides with said random number generated by said client, and sending an inquiry about start of a service to said service server based on a result of the confirmation about said random number ~~according to claim 16~~,

wherein when re-ciphering said deciphered random number, said service server not only re-ciphers said deciphered random number but also ciphers a code indicating said service server, and transmits said re-ciphered random number and said code thus ciphered to said client~~;~~, and

wherein when re-deciphering said re-ciphered random number, said client not only re-deciphers ~~aid~~said re-ciphered random number but also deciphers ~~aid~~said ciphered code, confirms whether a service server which transmitted said re-ciphered random number and said ciphered code coincides with said service server to which said client transmitted said ciphered random number, and ~~sending~~sends said inquiry about start of said service to said service server, based on a result of the confirmation about said service server.

B1

18. (currently amended)A computer program for use in performing authentication between a client and a service server connected over a network, comprising the steps of:

generating, by said client, a random number, ciphering said random number, and transmitting said random number thus ciphered to said service server;

deciphering, by said service server, said ciphered random number transmitted from said client, re-ciphering said random number thus deciphered, and transmitting said random number thus re-ciphered to said client; and

re-ciphering, by said client, said re-ciphered random number, confirming whether said random number thus re-deciphered coincides with said random number generated by said client, and sending an inquiry about start of a service to said service server based on a result of the confirmation about said random number,

wherein when re-ciphering said deciphered random number, said service server not only re-ciphers said deciphered random number but also ciphers a code

indicating said service server, and transmits said re-ciphered random number and said code thus ciphered to said client, and

wherein when re-deciphering said re-ciphered random number, said client not only re-deciphers said re-ciphered random number but also deciphers said ciphered code, confirms whether a service server which transmitted said re-ciphered random number and said ciphered code coincides with said service server to which said client transmitted said ciphered random number, and sends said inquiry about start of said service to said service server, based on a result of the confirmation about said service server.

B1

19. (currently amended)An authentication system comprising:

a client; and

a service server connected over a network,

wherein said client generates a random number, ciphers said random number, and transmits said random number thus ciphered to said service server,

wherein said service server deciphers said ciphered random number, re-ciphers said random number thus deciphered, and transmits said random number thus re-ciphered to said client, ~~and~~

wherein said client re-deciphers said re-ciphered random number, confirms whether said random number thus re-deciphered coincides with said random number generated by said client, and sends an inquiry about start of a service to said service server based on a result of the confirmation about said random number,

wherein when re-ciphering said deciphered random number, said service server not only re-ciphers said deciphered random number but also ciphers a code indicating said service server, and transmits said re-ciphered random number and said code thus ciphered to said client, and

wherein when re-deciphering said re-ciphered random number, said client not only re-deciphers said re-ciphered random number but also deciphers said ciphered code, confirms whether a service server which transmitted said re-ciphered random number and said ciphered code coincides with said service server to which said client transmitted said ciphered random number, and sends said inquiry about start of said service to said service server, based on a result of the confirmation about said service server.

20. (previously presented) A method for performing authentication between a first computer and a second computer connected over a network, comprising the steps of:

transmitting, by said first computer, a service request to said second computer, a certificate being attached to said service request;

generating, by said second computer, a ciphering key according to a result of confirmation of said certificate transmitted from said first computer, ciphering said ciphering key with a public key of said first computer, and transmitting said ciphering key thus ciphered to said first computer;

generating, by said first computer, a random number, deciphering said ciphered ciphering key, ciphering said random number with said ciphering key thus

deciphered, and transmitting said random number thus ciphered to said second computer;

deciphering, by said second computer, said ciphered random number, re-ciphering said random number thus deciphered and ciphering a code indicating said second computer both using a private code of said second computer, and transmitting said random number thus re-ciphered and said code thus ciphered to said first computer; and

re-deciphering, by said first computer, said re-ciphered random number and deciphering said ciphered code both using a public key of said second computer, confirming whether said re-deciphered random number coincides with said random number generated by said first computer and whether said code thus deciphered is valid, and sending an inquiry about start of a service based on results of the confirmation about said random number and the confirmation about said code.

21. (previously presented) The method according to claim 20, wherein said ciphering key is a session key.

22. (previously presented) The method according to claim 20, wherein said code indicating said second computer is either one of a name of said second computer and a certificate of said second computer.

23. (previously presented) A computer program for use in performing authentication between a first computer and a second computer connected over a network, comprising the steps of:

transmitting, by said first computer, a service request to said second computer, a certificate being attached to said service request;

generating, by said second computer, a ciphering key according to a result of confirmation of said certificate transmitted from said first computer, ciphering said ciphering key with a public key of said first computer, and transmitting said ciphering key thus ciphered to said first computer;

generating, by said first computer, a random number, deciphering said ciphered ciphering key, ciphering said random number with said ciphering key thus deciphered, and transmitting said random number thus ciphered to said second computer;

deciphering, by said second computer, said ciphered random number, re-ciphering said random number thus deciphered and ciphering a code indicating said second computer both using a private code of said second computer, and transmitting said random number thus re-ciphered and said code thus ciphered to said first computer; and

re-deciphering, by said first computer, said re-ciphered random number and deciphering said ciphered code both using a public key of said second computer, confirming whether said re-deciphered random number coincides with said random number generated by said first computer and whether said code thus deciphered is

valid, and sending an inquiry about start of a service based on results of the confirmation about said random number and the confirmation about said code.

24. (previously presented) An authentication system comprising:

a first computer; and

a second computer connected over a network,

wherein said first computer transmits a service request to said second computer, a certificate being attached to said service request,

B1

wherein said second computer generates a ciphering key according to a result of confirmation of said certificate transmitted from said first computer, ciphers said ciphering key with a public key of said first computer, and transmits said ciphering key thus ciphered to said first computer,

wherein said first computer generates a random number, deciphers said ciphered ciphering key, ciphers said random number with said ciphering key thus deciphered, and transmits said random number thus ciphered to said second computer,

wherein said second computer deciphers said ciphered random number, re-ciphers said random number thus deciphered and ciphers a code indicating said second computer both using a private code of said second computer, and transmits said random number thus re-ciphered and said code thus ciphered to said first computer, and

wherein said first computer re-deciphers said re-ciphered random number and deciphers said ciphered code both using a public key of said second computer,

confirms whether said re-deciphered random number coincides with said random number generated by said first computer and whether said code thus deciphered is valid, and sends an inquiry about start of a service based on results of the confirmation about said random number and the confirmation about said code.